2007 International Symposium on Nonlinear Theory and its Applications
NOLTA'07, Vancouver, Canada, September 16-19, 2007

Optimal Spreading Sequences for Chaos-Based Communication Systems

T. Papamarkou† and A.J. Lawrance†

†Department of Statistics, University of Warwick
Coventry, CV4 7AL, UK
Email: T.Papamarkou@warwick.ac.uk, A.J.Lawrance@warwick.ac.uk

Abstract—As a continuation from [2], some higher-order statistical dependency aspects of chaotic spreading sequences used in communication systems are presented. The autocorrelation function (ACF) of the mean-adjusted squares, termed the quadratic autocorrelation function, forms the building block of nonlinear dependence assessment of the family of spreading sequences under investigation. Explicit results are provided for the theoretical lower bound, the so-called Fréchet lower bound, of the quadratic ACF of that family. A method for producing a spreading sequence which attains the Fréchet bound is introduced.

Key Words—quadratic autocorrelation, negative statistical dependency, Fréchet lower bound, chaos communication systems

1. Introduction

In seeking to meet the minimum bit energy criterion for chaos communications Yao, [4], focused on spreading sequences with negative non-linear dependency and Lawrance and Papamarkou, [2], defined the deformed circular map as an effective candidate for generating carrier signals. For more general information about chaos communications see the monograph by Lau and Tse, [1]. The main requirement of the criterion for optimality is to achieve a value for the first lag of quadratic ACF as close as possible to -1. Since the achieved optimal choice is the deformed circular map with deforming parameter $r = 0.42$, whose $lag(1)$ quadratic ACF equals -0.722, there arises the question as to how near is -0.722 to the theoretical lower bound. It is known (see Ripley, [3]) that there exists such a correlation lower bound over all bivariate distributions with a specified marginal distribution; it is called the Fréchet lower bound.

The Fréchet lower bound of the $lag(1)$ quadratic ACF is calculated for the family of marginal distributions

$$f(x) = \begin{cases} -2(1-r)x, & -1 \le x \le 0 \\ 2rx, & 0 < x \le 1 \end{cases}, \qquad (1)$$

which is the class of invariant densities $f(x)$ of any deformed circular map with deforming parameter $r \in (0, 1)$.

Such a result gives further insight to the problem of optimal spreading in chaos-based communication systems by revealing the fact that the the lower bound equals -0.968 when $r = 0.42$ and -1 when $r = 0.5$. The latter case implies that the lower extreme of -1 can be attained by appropriately choosing the spreading sequence.

Bernoulli circular spreading is introduced as a scheme for producing carrier signals that attain the -1 Fréchet bound of $lag(1)$ quadratic ACF.

2. Fréchet Lower Bound of Deformed Circular Map

2.1. Deformed Circular Map

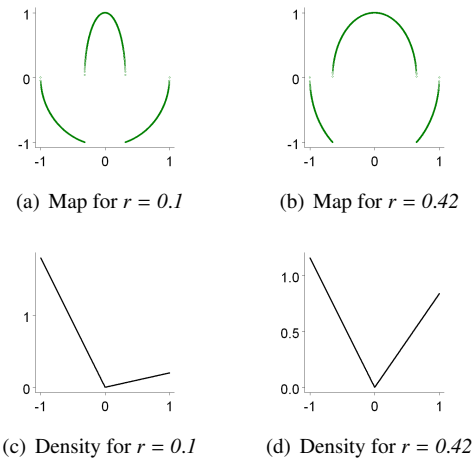
A recap on the *deformed circular map* (see Lawrance and Papamarkou, [2]) follows due to its central role in our analysis. It is defined as $\tau(x) =$

$$\begin{cases} -\sqrt{-(1-r)^{-1}x^2 + (1-r)^{-1}}, & -1 \le x < -\sqrt{r} \\ \sqrt{-r^{-1}x^2 + 1}, & -\sqrt{r} \le x < \sqrt{r} \\ -\sqrt{-(1-r)^{-1}x^2 + (1-r)^{-1}}, & \sqrt{r} \le x \le 1 \end{cases}, \qquad (2)$$

where the *deforming parameter* $r \in (0, 1)$ determines the range of each branch.

The invariant density $f(x)$ of the map is given by (1).

Figure 1 displays two representative examples of deformed circular maps as well as their associated invariant densities.



(a) Map for $r = 0.1$ (b) Map for $r = 0.42$

(c) Density for $r = 0.1$ (d) Density for $r = 0.42$

Figure 1: Two examples of deformed circular maps and their invariant densities.

The graph of $lag(1)$ quadratic ACF as a function against the deforming parameter r is represented by the dotted-dashed line of Figure 2.

2.2. Calculation of Fréchet Lower Bound

The main idea for calculating the Fréchet lower bound lies in the fact that for any pair of random variables (r.v.) (Y, W) with marginal cumulative distribution functions (c.d.f) $F_Y(\cdot)$, $F_W(\cdot)$ and inverse c.d.f's $F_Y^{-1}(\cdot)$, $F_W^{-1}(\cdot)$, the minimum correlation is that of the variables $F_Y^{-1}(U)$ and $F_W^{-1}(1-U)$, where U is a $\mathbb{U}(0,1)$ random variable. This becomes clearer if we think that:

• any two random variables U and $1-U$ have the minimum correlation, that is $Corr(U, 1-U) = -1$,

• if $U \sim \mathbb{U}(0,1)$, then $1-U \sim \mathbb{U}(0,1)$ and

• according to the inverse transformation of a uniformly distributed variable $U \sim \mathbb{U}(0,1)$, it holds that for any c.d.f. F the r.v. $Y := F^{-1}(U)$ is continuous with c.d.f. $F(y)$.

For the facilitation of notation, set

$$Z := (X-\mu)^2, \tag{3}$$

where $\mu = E(X)$ is the mean of the stationary carrier signal.

By using the previous remarks, it is deduced that

$$(X_t-\mu)^2 \sim F_Z^{-1}(U),\ (X_{t-1}-\mu)^2 \sim F_Z^{-1}(1-U), \tag{4}$$

which means that

$$E\left[(X_t-\mu)^2(X_{t+1}-\mu)^2\right] = \int_0^1 F_Z^{-1}(u)F_Z^{-1}(1-u)\,du. \tag{5}$$

The stationarity assumption for the spreading sequence allows for the marginal notation $X_t \equiv X,\ \forall t$, and combined with the definition of correlation leads to

$$Corr\left[(X_t-\mu)^2, (X_{t+1}-\mu)^2\right] = \frac{E\left[(X_t-\mu)^2(X_{t+1}-\mu)^2\right]^2 - [Var(X)]^2}{Var\left[(X-\mu)^2\right]}. \tag{6}$$

Equations (5) and (6) then yield

$$Corr\left[(X_t-\mu)^2, (X_{t+1}-\mu)^2\right] = \frac{\int_0^1 F_Z^{-1}(u)F_Z^{-1}(1-u)\,du - [E(Z)]^2}{Var(Z)}. \tag{7}$$

$E(Z)$ and $Var(Z)$ that appear in (7) are linear functions of the first four moments $E(X^i),\ i \in 1,2,3,4$, which in turn can be easily expressed as polynomials of the deforming parameter r. Hence, for the computation of the $lag(1)$ quadratic ACF to be accomplished the calculation of the integral of formulae (7) is required. The inverse c.d.f. $F_{(X-\mu)^2}^{-1}$ of $(X-\mu)^2$ is needed for the computation of the integral.

An analytic expression has been found for $F_{(X-\mu)^2}^{-1}$:

• For $0 < r < \frac{1}{8}$, $F_{(X-\mu)^2}^{-1}(x) =$

$$\begin{cases} \left[\dfrac{x}{4\mu(\mu+1)(r-1)}\right]^2, & 0 \le x < 4\mu(\mu+1)(r-1) \\ \left(\sqrt{\dfrac{x+r-1}{r-1}}+\mu\right)^2, & 4\mu(\mu+1)(r-1) \le x < 1-r \\ \left(\sqrt{\dfrac{x+r-1}{r}}-\mu\right)^2, & 1-r \le x < 1 \end{cases} \tag{8}$$

• For $r = \frac{1}{8}$ or $r = \frac{7}{8}$, $F_{(X-\mu)^2}^{-1}(x) =$

$$\begin{cases} \left(\dfrac{4x}{7}\right)^2, & 0 \le x < \dfrac{7}{8} \\ \left(\sqrt{8x-7}+\dfrac{1}{2}\right)^2, & \dfrac{7}{8} \le x < 1 \end{cases} \tag{9}$$

• For $\frac{1}{8} < r < \frac{1}{2}$, $F_{(X-\mu)^2}^{-1}(x) =$

$$\begin{cases} \left[\dfrac{x}{4\mu(r-1)}\right]^2, & 0 \le x < 4\mu^2(1-r) \\ \left[(\mu(1-2r)+\right. & 4\mu^2(1-r) \le x < \\ \left.+\sqrt{4\mu^2r(r-1)+x}\right]^2, & 4\mu(\mu+1)r+1 \\ \left(\sqrt{\dfrac{x+r-1}{r}}-\mu\right)^2, & 4\mu(\mu+1)r+1 \le x < 1 \end{cases} \tag{10}$$

• For $r = \frac{1}{2}$,

$$F_{(X-\mu)^2}^{-1}(x) = x,\ 0 \le x < 1 \tag{11}$$

• For $\frac{1}{2} < r < \frac{7}{8}$, $F_{(X-\mu)^2}^{-1}(x) =$

$$\begin{cases} \left[\dfrac{x}{4\mu r}\right]^2, & 0 \le x < 4\mu^2 r \\ \left[(\mu(1-2r)+\right. & 4\mu^2 r \le x < \\ \left.+\sqrt{4\mu^2r(r-1)+x}\right]^2, & r-(r-1)(2\mu-1)^2 \\ \left(\sqrt{\dfrac{x-r}{1-r}}+\mu\right)^2, & r-(r-1)(2\mu-1)^2 \le x < 1 \end{cases} \tag{12}$$

• For $\frac{7}{8} < r < 1$, $F_{(X-\mu)^2}^{-1}(x) =$

$$\begin{cases} \left[\dfrac{x}{4\mu r}\right]^2, & 0 \le x < 4\mu(1-\mu)r \\ \left(\sqrt{\dfrac{r-x}{r}}-\mu\right)^2, & 4\mu(1-\mu)r \le x < r \\ \left(\sqrt{\dfrac{x-r}{1-r}}+\mu\right)^2, & r \le x < 1 \end{cases} \tag{13}$$

Having obtained the inverse c.d.f. F_Z^{-1} analytically, the integral $\int_0^1 F_Z^{-1}(u)F_Z^{-1}(1-u)\,du$ can be found numerically. Then, (7) gives the minimal attainable $lag(1)$ quadratic ACF of the family of deformed circular maps as a function of r, which corresponds to the solid line of Figure 2.

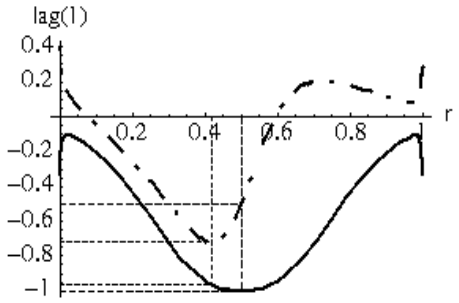


Figure 2: Dotted-dashed line: Plot of the *lag(1)* quadratic ACF of the deformed circular map versus its deforming parameter r. Solid line: Fréchet lower bound of the *lag(1)* quadratic ACF for the class of spreading sequences with invariant density given by (1).

2.3. Conclusions from Fréchet Lower Bound

The best match for the optimality criterion among the family of deformed circular maps, that is the one with $r = 0.42$, has *lag(1)* quadratic ACF equal to -0.722. Comparing this value to the corresponding Fréchet lower bound of -0.968 (see Figure 2), we could claim that although the specific map outperforms others traditionally used for producing carrier signals, there may still be a map or method which produces better spreading sequences with respect to the optimality criterion.

There is another result of engineering importance though, which refers to the case $r = 0.5$. If we choose from the class of distributions (1) to give the invariant density $f(x)$ of the spreading sequence

$$(X_0, X_1, X_2, \ldots, X_n) \tag{14}$$

as

$$f(x) = \begin{cases} -x, & -1 \le x \le 0 \\ x, & 0 < x \le 1 \end{cases}, \tag{15}$$

then the Fréchet lower bound of the *lag(1)* quadratic ACF of (14) equals -1. In other words, there may exist a way of producing a carrier signal (14) with invariant density described by (15) which fulfils the optimality criterion, and this is our aim.

3. Attaining the Lower Bound of -1

3.1. Problem Set-Up

We sample from (14), but our interest focuses on

$$\Big((X_1 - \mu)^2, (X_2 - \mu)^2, \ldots, (X_n - \mu)^2\Big), \tag{16}$$

where μ denotes the mean of (14).

For ease of notation, we set

$$Z_i := (X_i - \mu)^2,\ i \in \{1, 2, \ldots, n\}. \tag{17}$$

Under the new notation, we can refer to (14) as

$$\Big(Z_1, Z_2, \ldots, Z_n\Big). \tag{18}$$

The second order ACF of (14) is nothing but the first order ACF of (18). So, we could restate our goal; we want to find a sequence (14) with invariant density (15) such that the stationary random sequence (18) has linear ACF with value -1 for its first lag.

3.2. Solution: Bernoulli Circular Spreading

The solution comes from the remark that the linear correlation of two random variables Z_{i-1}, Z_i can be -1 if they are linearly related and choose

$$Z_i = -Z_{i-1} + 1. \tag{19}$$

The equations (17) and (19) imply

$$(X_i - \mu)^2 = 1 - (X_{i-1} - \mu)^2. \tag{20}$$

and (20) implies

$$X_i = \mu \pm \sqrt{1 - (X_{i-1} - \mu)^2}. \tag{21}$$

As it can be seen from (21), the complication is that for each value of X_{i-1} there exist two possible choices for X_i that lie on circle (20). In other words, we can't define a map τ and use it to generate a spreading sequence whose members lie on circle (20).

We abandon the idea of using a chaotic map to produce sequence (14). Our proposal is to decide randomly which of the two possible values of X_i to use in each step. The $\pm$ sign of (21) could be seen as a random variable A_i:

$$A_i = +1 \Rightarrow X_i = X_i^u := \mu + \sqrt{1 - (X_{i-1} - \mu)^2}, \tag{22}$$

$$A_i = -1 \Rightarrow X_i = X_i^\ell := \mu - \sqrt{1 - (X_{i-1} - \mu)^2}. \tag{23}$$

Figure 3 visualizes our suggestion:

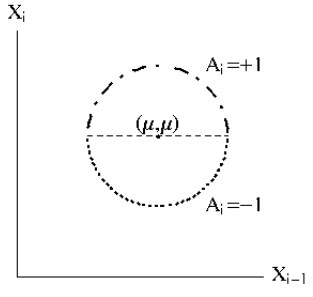


Figure 3: If $A_i = +1$, we choose the value of X_i from the upper cemi-circle (dotted-dashed line), whereas if $A_i = -1$, from the lower cemi-circle (dotted line).

In that way, we defined a random sequence

$$(A_1, A_2, \ldots, A_n). \tag{24}$$

We assume that (24) is a sequence of identically distributed random variables. More specifically, we assume that

$$A_i \sim Ber(p),\ i \in \{1, 2, \ldots, n\}, \tag{25}$$

where p is the probability that $A_i = +1$. Equation (21) can now be rewritten as

$$X_i = \mu + A_i \sqrt{1 - (X_{i-1} - \mu)^2}, \tag{26}$$

where A_i is described by (25). Under a more general notation, we could write

$$\tau(X) = \mu + A \sqrt{1 - (X - \mu)^2}. \tag{27}$$

where τ doesn't refer to a map anymore but to a geometrical shape, a circle.

We define the Bernoulli spreading sequence to be a carrier signal produced by the set of equations (25), (26).

3.3. Stationarity of Bernoulli Circular Spreading

The proposed spreading sequence is stationary. In order to check the form of its marginal distribution, a modified version of the Perron-Frobenius equation (P-F) must be set and then it can be shown that (15) is a solution of the P-F equation.

We start from the general case of a circle with centre $(k, k),\ k \in \mathbb{R}$, and radius 1:

$$(X_i - k)^2 + (X_{i-1} - k)^2 = 1. \tag{28}$$

Note that at this point the centre of the circle is based on an arbitrary real number k, the mean $\mu \equiv E(X)$ of (14) is not invoked here.
Then we define X_i sequentially

$$X_i = k + A_i \sqrt{1 - (X_{i-1} - k)^2}, \tag{29}$$

where A_i is defined by (25) with

$$p = P(A = +1),\ 1 - p = P(A = -1). \tag{30}$$

Alternatively, we write

$$\tau(X) = k + A \sqrt{1 - (X - k)^2}. \tag{31}$$

and, after solving,

$$\tau(g_i^\tau(x)) = x \tag{32}$$

we find the 'pre-images' $g_i^\tau(x)$ of x:

$$g_1^\tau(x) := k - \sqrt{1 - (x - k)^2},\ g_2^\tau(x) := k + \sqrt{1 - (x - k)^2}. \tag{33}$$

We have proved that under the Bernoulli scheme the adapted Perron-Frobenius equation is $f(x) =$

$$\begin{cases} (p-1) g_1^\tau{}'(x)[f(g_1^\tau(x)) + f(g_2^\tau(x))], & k - 1 \le x \le k \\ p\, g_1^\tau{}'(x)[f(g_1^\tau(x)) + f(g_2^\tau(x))], & k < x \le k + 1 \end{cases}. \tag{34}$$

If we restrict ourselves in the case $p = 0.5$, equation (34) then takes the form $f(x) =$

$$\begin{cases} -\frac{1}{2}\, g_1^\tau{}'(x)[f(g_1^\tau(x)) + f(g_2^\tau(x))], & k - 1 \le x \le k \\ \\ \frac{1}{2}\, g_1^\tau{}'(x)[f(g_1^\tau(x)) + f(g_2^\tau(x))], & k < x \le k + 1 \end{cases}. \tag{35}$$

It is a routine check to verify that for $p = 0.5$ the function

$$f(x) = \begin{cases} -x + k, & k - 1 \le x \le k \\ x - k, & k < x \le k + 1 \end{cases} \tag{36}$$

satisfies (35) and that the mean of the resulting stationary spreading sequence is

$$E(X) = k. \tag{37}$$

4. Conclusions and Further Work

It is interesting to comment on the case of the unit circle (the circle of radius 1 centered at the origin $(0, 0)$). In that case, $k = 0$, equations (36) and (37) show that the spreading sequence is characterized by the invariant density (15) and has mean $E(x) = 0$. So the invariant density of the Bernoulli circular spreading coincides with the one of the deformed circular map with deforming parameter $r = 0.5$. However, these two methods differ in their quadratic dependency; the $lag(1)$ quadratic ACF of the deformed circular map with $r = 0.5$ equals -0.5, whereas our approach is optimal in the sense that it attains the Fréchet lower bound of all random sequences with invariant density given by (15), which is -1.

This paper deals with work-in-progress. It has been proven that the BER of a Bernoulli circular spreading of length N, where N is any even natural number, coincides with the lower bound of BER. It has also been shown that the lower bound of BER is not attained for spreading of odd length N. Simulations confirm our proof. Further analysis and simulations of the Bernoulli circular spreading are being carried out to examine the BER properties and engineering applicability of the proposed spreading method.

Acknowledgments

We would like to thank the NOLTA2007 organizing committee for giving us the opportunity to present this work.

References

[1] F. C. M. Lau & C. K. Tse, *Chaos-Based Digital Communication Systems: Operation, Analysis and Evaluation*, 1st ed, Heidelberg, NJ: Springer-Verlag, 2003.

[2] A. J. Lawrance & T. Papamarkou, "Higher Order Dependency of Chaotic Maps," *NOLTA 2006 Proceedings, IEICE*, pp.695–698, 2006.

[3] B. D. Ripley, "Stochastic Simulation", *Wiley Series in Probability and Mathematical Statistics*, 1987.

[4] J. Yao, "Optimal chaos shift-keying communications with correlation decoding," *ISCAS04, International Society for Circuits and Systems conference*, Vancouver 23-26 May 2004, IV, pp.593–596.